HOW

TO MANAGE ENTERPRISE RISK VIA CERTIFICATION OF MANAGEMENT SYSTEMS

BUREAU VERITAS

RISK MANAGEMENT
for a fast-changing world

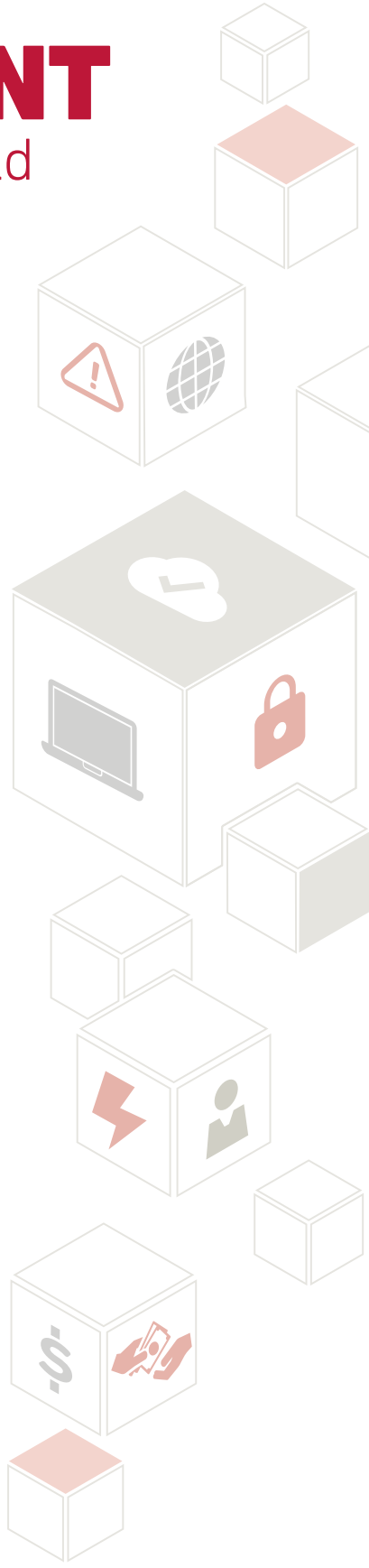
Contents

Businesses today face more risk than ever before. The digitalization of assets, products and services creates opportunities but also threatens cyber security. Governments have introduced regulations on issues ranging from data protection to bribery. And traditional threats to business continuity such as utility interruptions are compounded by our growing dependence on digital networks.

Companies tend to manage the risks they understand, such as financial and commercial risk. But the emerging, complex nature of other threats, in particular those relating to data, assets and people, means they often slip below many managers' radar.

A comprehensive strategy is needed, first to identify risks to business, then to manage them via the adoption of consistent processes within a systematic framework. This is the only way to achieve a 360° vision of risks, foster a proactive culture of risk management, safeguard your reputation, secure stakeholder trust, and protect performance.

This white paper outlines a holistic approach for addressing enterprise risk to meet the specific needs of your organization.



5 RISKS
keep managers up at night

1 **78%** **INFORMATION SECURITY**

2 **78%** **BUSINESS CONTINUITY**

3 **68%** **PROTECTION OF CLIENT DATA**

4 **53%** **POOR PROTECTION OR USE OF ASSETS**

5 **52%** **BRIBERY OF EMPLOYEES OR SUPPLY CHAIN**

THEY ARE DRIVEN BY
2 MAIN CONCERNS

REPUTATION

is the key driver
when thinking about:

Protection of client data **40%**

Information systems security **36%**

BUSINESS PERFORMANCE

is the key driver for

Business continuity **73%**

Asset management risks **67%**

COMPANIES HAVE STARTED TO
ADDRESS THESE RISKS

6 in 10

companies have one or more policies or procedures in place covering:

- **Data protection**
- **Information systems security**
- **Business continuity**

4 in 10

companies have implemented:

- **An information security management system:** **ISO 27001**

and / or

- **A business continuity management system:** **ISO 22301**

1 in 3

companies manage their information systems security via certification to **ISO 27001** or a similar standard

Certification of Enterprise Risk management systems brings

3 KEY ADVANTAGES

Ensure CONSISTENT IMPLEMENTATION of your management systems

Target COMPLIANCE and safeguard reputation

Achieve CONTINUOUS IMPROVEMENT

Based on a survey carried out by Bureau Veritas in Summer 2017

DESIGNING A COMPREHENSIVE FRAMEWORK
to manage Enterprise Risk

EVERY BUSINESS ACTIVITY INVOLVES SOME RISK.

Organizations identify, monitor and manage risks they deem business-critical. These are typically headed by financial, market and regulatory risk with operational risks such as safety and supply chain considered more or less critical depending on the nature of the business. Catastrophic events such as extreme weather and power outages are also considered.

But in today's fast-changing world, the potential impact and likelihood of risks traditionally grouped under operational or regulatory risk or catastrophic events are growing (see p.5). Companies must contend with the threat of cyber-attacks and IT outages, and their potential impact on reputation and business continuity. Regulation has increasingly bigger teeth, particularly in areas such as anti-bribery and data protection. Conversely, in a fiercely competitive environment, superior performance can be gained from proactive management of business assets.

TAKING A 360° VIEW WITH A COMPREHENSIVE RISK MANAGEMENT FRAMEWORK

The sheer volume and complexity of these emerging risks makes it hard for managers to stay up to date with threats facing their organization. That is why effective risk management is best achieved through a comprehensive framework that provides the foundations and arrangements to embed it throughout the organization at all levels.

Risk management cannot be a stand-alone activity, separate from the company's main processes. It must be led by senior management and integral to the entire organization, including strategic planning and project and change management processes. It must also be tailored to the organization and its context. For a high street bank, protection of client data is likely to be among its top risks. Asset management is a bigger concern for an industrial manufacturer or power generator than, say, for an advertising agency.

No framework is set in stone: it must respond to external and internal events and changes in context and knowledge. As threats and opportunities emerge, or gain in importance, risk managers need to be able to monitor, review and reassess the framework in place, ensuring it stays dynamic, iterative and relevant.

By developing, implementing and continuously improving a framework to integrate risk management into the organization's overall governance, strategy, planning, reporting processes, policies, values and culture, businesses ensure that risk management decisions are based on the best available information. This helps decision makers make informed choices, prioritize actions, distinguish among alternative courses of action, and create accountability.

The sheer volume and complexity of these emerging risks makes it hard for managers to stay up to date with threats facing their organization.

Prioritizing risk

CYBER SECURITY IS THE MOST IMPORTANT EMERGING ENTERPRISE RISK FOR MAJOR COMPANIES

To see how leading companies prioritize risks, we looked at the Principal Risks outlined by a selection of 10 FTSE 100 companies[1]. Our objectives were to see which risks are the most frequently cited, and whether emerging Enterprise Risks[2] were considered to be Principal Risks and addressed as such.

The diagram below shows the risks identified across the sample[3]. For clarity, we have grouped these under common headings. As might be expected, the most frequent risks faced by companies related to those with the potential to directly impact sales and profits: regulatory, market, macro, and operational risks.

Interestingly, information security and cyber security followed swiftly behind this. They were cited by nine of the 10 companies studied[4]: one company cited IT reliability as an additional information security risk.

Other emerging Enterprise Risks were cited regularly, but not always as a standalone risk. Anti-bribery was frequently mentioned as part of regulatory compliance, but rarely as a standalone risk. Business continuity was cited by 7 of the 10 companies in explanations of risks such as operations or information security. Asset management was the least mentioned Enterprise Risk.

ABOUT THE SAMPLE

The companies we selected came from a range of sectors: real estate and financial services, mining, oil and gas, pharmaceuticals, transport and aerospace, telecoms, media and advertising, retail, food. All are multinational companies. The average number of risks identified by each company was 10.7.

- Emerging Enterprise Risks that can be addressed through new certifications mentioned in this white paper
- Risks that can be addressed through existing certification schemes, emissions verification and assurance of sustainability report services
- Other risks

[1] Listed UK companies are required to analyze and disclose their Principal Risks as part of their Annual Report, including those that would threaten its business model, future performance, solvency or liquidity.

[2] Cyber security, personal data protection, business continuity, asset management, anti-bribery

[3] Risks in the diagram are ranked by size but are not to scale

[4] Listed by one company under "Catastrophic Risk"

DESIGNING A COMPREHENSIVE FRAMEWORK
to manage Enterprise Risk

USING CERTIFICATION TO MANAGE SPECIFIC RISKS

One conundrum that businesses often face is how to manage operational risks throughout the organization once they have been identified as critical within the risk management framework.

In this context, implementation and certification of an internationally recognized management system for each critical risk, provides a useful way to bridge the gap between high-level ambition and the day-to-day processes and mindset required to manage each risk.

Implementing a management system to manage risk safeguards your business, reducing threats to profits, performance and reputation. Certification meanwhile inspires trust in your leadership, among both staff and external stakeholders. It helps prove compliance with legislation and internationally recognized criteria and communicates transparency and a commitment to excellence. Moreover, should breaches occur, certification demonstrates due diligence and, in some cases, can allow you to mitigate penalties.

Identification of business-critical risks is achieved through the comprehensive monitoring enabled by a rigorous framework; individual certifications then ensure that potent threats to the organization are correctly anticipated.

How does this work in practice? In the example given earlier, the management of the high street bank may choose to certify its management systems or adopt a technical standard to address information security and business continuity as these are identified as pressing threats. It may also decide to monitor the context via the risk management framework to assess the need for anti-bribery and data protection certifications further down the line.

By first mapping the risks that apply to your organization, and then putting in place the appropriate certifications to address them, your business can take crucial steps on the road to more resilient business performance – and greater peace of mind.

Identification of business-critical risks is achieved through the comprehensive monitoring enabled by a rigorous framework; individual certifications then ensure that potent threats to the organization are correctly anticipated.

CERTIFICATIONS
focusing on business-critical risks

International certification standards have been used for 30 years to address many areas of risk, starting with quality (ISO 9001) and environmental management (ISO 14001). The next generation of risk mangement systems include Information Security, Business Continuity, Asset Management and Anti-Bribery, which Bureau Veritas groups as its Enterprise Risk portfolio. A fifth, Data Protection can be managed via a technical standard developed by Bureau Veritas.

INFORMATION SECURITY: ISO 27001 ISMS

In today's technologically dependent world, the threat of information security breaches is growing. A single incident can impact your company's image, business continuity, and revenues. Large organizations have long been regular targets of attacks, but small- to medium-sized companies are increasingly at risk. As such, organizations are facing more stringent regulation, and stakeholder expectations for data security are high. That is why more and more organizations are seeing the value of a structured approach to information security such as that provided by ISO 27001.

By actively communicating your adherence to such an approach, certification allows you to provide transparency to your customers and demonstrate responsible handling of customer data. It reassures stakeholders that you are able to address the unique threats and complexities of the modern technological landscape, which enhances your reputation and differentiates you from competitors.

For more information **click here**.

> *Large organizations have long been regular targets of attacks, but small- to medium-sized companies are increasingly at risk.*

Certifications focusing on **BUSINESS-CRITICAL RISKS**

BUSINESS CONTINUITY: ISO 22301 BCMS

Utility services interruption, IT outages and breaches, acts of nature, supply chain disruption: in our uncertain world, these are just a few of the many threats that can harm – or end - your business by compromising your supply chain, quality standards, or the security of your organization.

To ensure you recover as quickly as possible after an incident, it is vital to establish a strategy to allocate responsibility and resources to understand the risks, plan for a crisis, create controls, and structure operations. By certifying to ISO 22301, your organization improves the resilience of the entire business ecosystem and society within which it operates. You also send a reassuring message to stakeholders by demonstrating that you can withstand and recover speedily from a crisis.

As well as enhancing your reputation, rapid recovery from incidents allows you to minimize risks to property, safeguard against revenue losses, and maintain cash flow. You ensure employee safety and reduce the risk of legal non-compliance.

For more information **click here**.

ASSET MANAGEMENT: ISO 55001 AMS

Successful management of your company's material and non-physical assets supports return on investment while helping you comply with health, safety and environmental requirements.

Implementation of the ISO 55001 management system standard helps you to balance risk against cost efficiency in decision-making, for example when setting priorities for asset maintenance. It contributes to reducing costs, boosting asset return on investment, and optimizing growth across the asset lifecycle – all of which result in improved performance and value creation.

ISO 55001 certification increases the value of one of your greatest assets: your reputation. Certification ensures transparency regarding appropriate use of funds and responsible asset management, sending a powerful message to stakeholders and differentiating you from other organizations. Certification also contributes to increasing profits by helping you identify opportunities for improvement and anchoring good asset management within your organization's culture.

For more information **click here**.

Certifications focusing on **BUSINESS-CRITICAL RISKS**

ANTI-BRIBERY: ISO 37001 ABMS

Corruption is a serious threat to any organization. Recent UN and OECD conventions aim at cracking down on bribery. As a result, 41 different countries have established anti-bribery laws*. Organizations whose representatives are found giving or receiving bribes will be subject to financial penalties, while directors risk personal criminal or civil liability.

The implementation of an ISO 37001-compliant management system establishes procedures to prevent, detect and manage the risk of bribery in your organization. Certification demonstrates compliance to legislation and shows transparency by opening you up to third party scrutiny of anti-bribery policies and processes.

In some countries, the presence of a compliance system is a direct legal requirement; in others, certification can demonstrate a company has taken proactive steps to prevent employees from engaging in bribery and show that any offences are the result of employee disobedience rather than a flawed company culture. ISO 37001 certification sends a clear message to your organization's stakeholders and the general public, encouraging trust and enhancing your reputation.

For more information **click here**.

**These include the US's Foreign Corrupt Practices Act and the UK's 2010 Bribery Act, both of which have transnational reach.*

> *Certification demonstrates compliance to legislation and shows transparency by opening you up to third party scrutiny of anti-bribery policies and processes.*

DATA PROTECTION: GDPR

To inspire trust in your data management, it is essential not only to implement appropriate management procedures, but also to achieve certification. The EU General Data Protection Regulation (already implemented and due to be enforced from May 25, 2018) tightens controls on companies dealing with EU citizens' data and imposes fines for non-compliance. In response to this, Bureau Veritas has developed a technical standard and voluntary certification program.

Implementing strong data management procedures limits the risk of potentially costly security breaches, safeguards customer privacy, and protects valuable data assets that are crucial to your business. Certification of your data protection procedures enables your organization to demonstrate your efforts to comply with regulations. As a result, should breaches occur, certification demonstrates due diligence and can help mitigate potential penalties.

For more information **click here**.

Bureau Veritas

TRAINING AND CERTIFICATION

Bureau Veritas' portfolio of Enterprise Risk Management services supports companies in protecting information systems and physical assets and proactively addressing emerging business risks.

CERTIFICATION

We have offered management systems certification to our clients since the first such international standard, ISO 9001 for quality, came into being in 1987.

Now recognized by over 40 national and international accreditation bodies across the world, Bureau Veritas holds United Kingdom Accreditation Service (UKAS) global accreditations for ISO 27001, ISO 55001 and ISO 22301 and has applied for ISO 37001.

TRAINING

Bureau Veritas also offers training courses to help understand the standards and how to apply them in your organization. Our training courses are delivered by lead auditors with years of industry experience and insight, who have been trained in interpersonal communication, intercultural issues and adult learning concepts:

CLASSROOM LEARNING

We offer a one-day introduction to each standard, a two-day mastering course for deeper information, a two-day internal auditor and a five-day lead auditor course.

E-LEARNING

A recent addition to our training offer, eLearning modules include awareness training, and specific modules on how to apply risk analysis methodologies or the context of the organization regarding the particular risk area.

BLENDED LEARNING

Blended learning packages combine components from a range of courses. Convenient eLearning modules help participants refresh and update knowledge first gained in the classroom.

Please note that course availability may vary by country. The Bureau Veritas website for your country contains more details on the classroom courses available locally.

For more detail on our Enterprise Risk portfolio of services visit our Enterprise Risk pages.

ABOUT BUREAU VERITAS

Bureau Veritas is a world leader in testing, inspection and certification. We help clients across all industries address challenges in quality, health & safety, environmental protection, enterprise risk and social responsibility. We support them in increasing performance throughout the life of their assets and products and via continuous improvement in their processes and management systems. Our teams worldwide are driven by a strong purpose: to preserve people, assets and the environment by identifying, preventing, managing and reducing risks.

For more information, contact Bureau Veritas:

Le Triangle de l'Arche
8 cours du Triangle
CS 90096
92937 Paris La Défense Cedex
FRANCE

certification.contact@bureauveritas.com

www.bureauveritas.com

Visit our Enterprise Risk pages

BUREAU VERITAS

Design and production: BOLDcie.com
Photo credits: Bureau Veritas / iStock / Thinkstock